Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing

Shane Horgan
Ben Collier
Richard Jones
Lynsay Shepherd

Horgan, S., Collier, B., Jones, R. & Shepherd, L. (2020) 'Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing', *Journal of Criminal Psychology*.
DOI: https://doi.org/10.1108/JCP-08-2020-0034

Reterritorialising the policing of cybercrime in the post-COVID-19 era: Towards a vision of local democratic cybercrime policing

Shane Horgan; Ben Collier; Richard Jones; Lynsay Shepherd

ACCEPTED MANUSCRIPT

Abstract

Design: This conceptual paper draws on empirical evidence from a range of sources (including official statistics) and the existing research literature, and revisits Routine Activities Theory in order to illuminate the way that cybercrime patterns are being transformed by the pandemic.

Purpose: Our purpose is to develop the theorisation of cybercrime in the context of the pandemic, and to sketch out a vision of how law enforcement might respond to a transformed landscape of online crime and offending.

Findings: The pandemic is reshaping the routine activities of societies en masse, leading to changes in the ecology of risk and opportunity for cybercrime. There is evidence of a significant increase in the prevalence of cybercrime as a result, yet much of this has a paradoxically 'local' character.

Implications: We identify specific practical implications for law enforcement, namely that the role of local police in policing cybercrime should be re-envisioned, with a democratic, community-oriented approach at its heart.

Value: The theoretical perspective outlined is a novel and critical development of a well-established framework, opening up new paths to the theorisation of cybercrime and cybercrime policing. Our suggestions for practitioners have the potential for direct impact, both at the level of practice, and in terms of broader imaginaries and organisation of police and policing.

1. Introduction

Crime, harm, and how societies police them are influenced by the cultural, economic and material factors present at particular points in history. In this article, we argue that modern societies have arrived at a transformative moment in which decades-long patterns of change are coming to fruition with important implications for cybercrime scholarship. Although this will undoubtedly become a trite observation, the emergence of a novel coronavirus in late 2019, and the subsequent global pandemic have caused transformative change to global societies and state institutions, with a rapidity unprecedented in modern history. As a result of these mass-scale social transformations, the coronavirus pandemic has been accompanied by a reshaping of the landscape of cybercrime and its place in broader patterns of harm and victimisation, and it is on this which we focus here. In order to make sense of these changes, we develop the argument, previously set out in Collier et al. (2020), that renewed approaches to theorising cybercrime are required in the context of the pandemic as it reveals many of the assumptions around the phenomenon of cybercrime and how it is policed do not necessarily hold true. The aims of this article are twofold: first, we explore, through an expanded approach to the criminological theorisation of online harms, how cybercrime is changing in the time of coronavirus. Secondly, building on this novel theoretical and empirical perspective, we propose a renewed role for local, democratic policing in the management of cybercrime.

We begin by considering how cybercrime is generally theorised in the criminological literature, discussing the oft-employed Routine Activities Theory (RAT) approach and the shortcomings of a too-narrow focus on the 'chemistry of crime' element. Tacking back to the Chicago School roots of RAT, we argue that a broader focus on the social ecology of crime has the potential to open up a renewed analytical perspective on cybercrime which is crucial in making sense of how cybercrime is changing in the pandemic. We then set out some of the emerging empirical evidence as to how the COVID-19 pandemic and government initiatives in response are creating novel cybercrime risks and opportunities for cybercrime markets. In the following section, we describe in broader terms how the pandemic is reshaping the routines of everyday life, and what this might mean for cybercrime victimisation, arguing that many of the issues that are emerging are of a particularly 'local' character. We then set out in detail our argument for a localised vision of cyber policing, showing how the unique strengths of local police forces might be well-positioned to address various aspects of the current model which may come under strain as a result of the pandemic, and drawing on the literature on democratic policing to identify the key principles that should inform this new capability. We conclude with some reflections as to the implications of our analysis for policymakers, practitioners, and the future of cybercrime scholarship.

2. Routine Activities Theory revisited

Cybercrime research has taken a particular interest in Routine Activities Theory (RAT) (Cohen and Felson, 1979), which it has employed to explain the presence or absence of crime online, drawing attention in particular to the convergence of motivated offender and suitable victim or target, and to how the anonymising and concealed nature of the Internet may generate frequent absences of 'capable guardianship'. This transformation of crime's relationship with space with the advent of the Internet has driven a large body of research which has applied this perspective (Wall, 2007), often from a microsociological perspective focusing on the interactions in time and space that do or do not present an 'opportunity' for an offender to commit crime; as such, these analyses bear theoretical similarities with perspectives associated with rational choice theory, situational crime prevention, and crime science.

The aim of Cohen and Felson's (1979) original article was to examine how deep structural changes in the spatial and temporal rhythms of the social fabric might account for changes in crime patterns, arguing that it was precisely such structural changes to society that had inadvertently produced the post-War increases in crime rates experienced in the United States.

In early work using the RAT framework, Cohen and Felson (1979) focused their attention on increases in affluence and various social transformations such as the movement of women into workplaces following the Second World War. These macro-social changes in the social structure were translated into a micro-level analytic framework, which proposed that when three particular factors - a motivated offender, a suitable target, and the absence of a capable guardian - converged in time and space, crime could occur. Cohen and Felson (1979) argued that the observed changes increased the number of homes without 'capable guardians' for longer periods of time which increased the possibility of a willing offender exploiting that 'vulnerable target'. The focus on materiality which this engenders, namely, the material and spatial components of targets (traditionally the weight and portability of consumer goods), the co-presence of victim and offender, and the ability of guardians to intervene in these processes, has generally made it a readily usable framework for making sense of cybercrime.

It is beyond the scope of this article to undertake a comprehensive review of RAT and cybercrime - for a more detailed review, see Reyns2018), however some key points are necessarily addressed below. In initial criminological forays into theorising cybercrime, one of the core debates animating this emerging field was around whether cybercrime constituted a distinctively 'novel' form of crime. There was a particular focus in these debates on the spatiality of the Internet and how this might transform crime and victimisation. By taking the various technological and infrastructural aspects of the Internet and rendering these as fundamental changes in social topology, RAT(which inherently conceives of crime through relations of space, time, and human behaviour) constituted a useful and reconciliatory way of making sense of online victimisation (Yar, 2005). In the criminological and sociological study of cybercrime, applications of RAT have focused on how the Internet maps on to these material-spatial arrangements; in particular how its 'hidden' and 'unregulated' qualities may frustrate capable guardianship. Ultimately, when criminologists have used RAT to make sense of the spatiality of the Internet, this has replicated the depictions of a global society with which the Internet was associated during its early years of commercialisation. arguing that it has exploded geographies of space into a hyperspatial online realm in which people from around the world are interconnected (Yar 2005; McGuire, 2007). Therefore RAT offers a straightforward way of thinking through the implications of the integration of the Internet into our everyday lives for crime and criminal justice - and as we argue here - for the social changes wrought by COVID-19, international lockdowns, and social distancing.

Applications of RAT that over-emphasise the situational causes of crime also effectively suggest straightforward and readily implementable crime prevention strategies. RAT has been applied to different forms of online offending and victimisation with varying degrees of profitability (see Reyns, 2018). Preoccupation with micro-level changes in human interactivity, connectivity, and what this means for 'criminal opportunity' has led to a focus predominantly on situational crime prevention perspectives associated with Newman and Clarke (2003). Until recently (see Maimon *et al*., 2019), this has arguably led to cybercrime research overlooking social perspectives on cybercrime prevention (Crawford, 2007), and how tertiary concepts such as 'collective efficacy', 'social capital', and community oriented models of policing might be re-envisaged and redeployed in this context. In the context of the pandemic, when the established times and spaces of the social are fundamentally challenged and reorganised, RAT provides a useful tool for the analysis of the increasingly fluid and dynamic micro and macro level implications of such a rapid exercises in social reorganisation that we are witnessing as the pandemic progresses.

Beyond the investigation of specific changes to routine activities, there has been some broader application of RAT to understanding the macro changes in crime with which the Internet is associated, casting it as a new and detached space in which crime may be committed. The base assumptions on which the criminological cybercrime canon has emerged are the same features on which earlier criminological accounts of the phenomenon expended so much ink; the features that separate it from terrestrial forms of crime. Cybercrime is, in this account, globalised in nature and 'despatialised' - unbounded by time or space, by city or sovereign spaces, and upends how the 'the crime problem' has been understood and tackled by nation states (for archetypal accounts see Yar and Steinmetz, 2019; Wall, 2007). The explosion of online offences in the past 20 years, along with prevalence of various forms of cybercrime victimisation among certain populations could thus be explained drawing on this perspective, where the Internet has facilitated globalised hyperconnectivity of vulnerable victims, willing offenders, and the absence of capable online guardians (Reyns, 2018; Williams, 2016; Leukfeldt and Yar, 2016; Holt and Bossler, 2008).

This characterisation of the Internet as a space unbounded in territory and time has tended to draw cybercrime scholarship towards a focus on the 'deterritorialisation' (Behr, 2008) of

crime problems and policing responses. In adopting this approach, analyses sought to avoid the limitations of criminological theory rooted in local or national boundaries, and highlighted its global nature and the challenges posed to sovereign criminal justice apparatus. By casting cybercrime problems as inherently international, unbounded by territory or jurisdiction, this 'deterritorialised' conceptualisation has generally also been useful for understanding the forms of cybercrime policing which subsequently have been developed in response. Cybercrime policing is indeed dominated by international relationships and networks, chiefly between centralised agencies such as the FBI (in the US) and NCA (in the UK); international co-operative organisations such as Interpol and Europol; and private sector providers. This has meant that the cybercrime response from law enforcement has been spearheaded by a mixture of 'high policing' and intelligence-led models focusing on 'serious cybercrime' in the hierarchy of standing (Yar, 2013), which have been leveraged for resourcing priority and symbolic prominence (Brodeur, 2010). Where 'low policing' has featured in academic and practitioner discussions, it mostly appears to be constructed in terms of its supportive capacity to the high policing agenda and investigative ends, generally in an intelligence-gathering role. In the UK this can be seen in the expansion of PREVENT-style policing to young 'at risk' online offenders (as, for example, in the NCA's 'Cyber choices' campaign).

Constructing the Internet, as this micro-situational approach generally does (Leukfeldt and Yar, 2016), as a place where guardianship is frustrated or impossible ignores the pervasive private sector cybersecurity industry, the power that Internet Service Providers have to screen and censor content, the vast surveillance capabilities of the security services, and the increasingly crucial role of platforms, such as Facebook and Google, in governing content and behaviour online. Many of these entities, institutions, and organisations have capacities of guardianship and control which would be inconceivable in pre-Internet societies, often in forms which take explicit account of local laws, jurisdictions, and cultural contexts.

Framing online crime as spatio-temporally unbounded also elides important aspects of the technical geography of the Internet and its control. Internet geography is far from the 'flat' space envisioned in early discussions of online space, and the material infrastructure of the Internet is often distributed in ways which are paradoxically local, as discussed in section 5 below. The influence of law and its enforcement, and the knock-on effect on hosting infrastructure, means that particular illicit services, whether they be for copyrighted material, illicit markets, or hosting tend to concentrate in jurisdictions where this content is not illegal or where the law is not enforced (Clayton, Moore, and Christin, 2015). In addition to this technical and legal geography, cybercrime and online harm are rooted in a local geography of cultures, practices, and concerns, and are as bound up in local communities as they are international ones. This is increasingly recognised by major Internet platforms, the de-facto capable guardians into whose hands much governance of online conduct falls, for example: issues at local and national level, such as the use of WhatsApp in India for casteist violence, the effects of disinformation on the US election, or the enforcement of strict German laws around the promotion of far-right ideology.

Consequently, , in focusing on the micro-level 'chemistry' of criminal opportunity, criminological analyses that draw on RAT have neglected to embrace the perspective's capacity to take into account wider impacts of macro-level social change, and their concomitant changes in social geography, like those originally identified by Cohen and Felson (1979). Although this micro-level focus in contemporary cybercrime scholarship elides the broader cultural, economic, and other macrosocial factors which attend crime, these shortcomings are not necessarily inherent to the broader theoretical framework. There is much worth salvaging in RAT, as its lens on the spatiotemporal determinants of crime is potentially particularly useful for making sense of the changes wrought by COVID-19, many of which directly affect peoples' daily routines. We argue that the sweeping changes our societies are facing are manifestly not only spatiotemporal, but also political, economic, and

cultural, much as the changes described by Cohen and Felson (1979) following the Second World War were. As is implicit in early RAT scholarship, the territories within which these micro-situations are composed are in fact themselves socially and historically contingent. Taking RAT back to these theoretical roots and connecting it up to these social forces therefore poses a potentially fruitful theoretical endeavour in the current context.

The roots of RAT as a theory of social ecology (in the mode of the Chicago School from which it emerged) including societal change, we contend, may therefore be more productive for developing more well-rounded understandings of cybercrime and online harm, especially in the context of mass-scale social changes such as those brought about or accelerated by the current pandemic. Societal responses to Covid-19 have accelerated already-ongoing changes to routine activities facilitated by information technology, and arguably, by returning to the original macro-level analytic approach of Cohen and Felson (1979), we can better understand these shifts in the context of longer-term social changes. It would appear r that 'lockdowns', physical distancing and other public health measures transform criminal and victimisation opportunity structures at the macro scale, decreasing the prevalence of some opportunities (e.g. domestic burglary), and increasing others (e.g. domestic violence, fraud, and cyber-dependent crime). These also reshape aspects of culture and social psychology in ways which are pertinent to understanding the changing nature of online harms.

We explore this further below and argue that this provides a productive way of making sense of how COVID is changing cybercrime, and help us reimagine the role of public policing. In doing so, we move beyond merely situational-level responses (which tend to reduce to measures such as target hardening and surveillance) towards approaches rooted in communities and social institutions, suggesting instead a more nuanced criminological and psychological understanding of cybercrime. In the following section, we consider some of the specific transformations prompted by the ongoing pandemic.

3. COVID and cybercrime: emerging evidence

Although it is undoubtedly far too early to pinpoint the lasting effects of the COVID-19 pandemic and the government responses it has prompted, at the time of writing a series of evidence sources have emerged which are suggestive of possible trends. The social, economic, and political consequences of lockdown, social distancing, and mass illness are becoming clearer, and evidence now suggests some large-scale transformation, at least in the short term, in patterns of crime. Below, we discuss some of the emerging evidence of how cybercrime appears to be changing as the pandemic progresses, drawing from a range of sources focused on the UK and the US by way of illustrating our wider theoretical argument. We begin by drawing evidence from official recorded crime figures, which indicate a transformation in crime patterns, then discuss in detail some of the broader indications we observe. In the subsequent section we discuss in broader, more theoretical terms, what this may mean for cybercrime in the long term.

Official government data on cybercrime is sparse in the United Kingdom for well-established reasons (Levi *et al*., 2017; Yar and Steinmetz, 2020), but sources are gradually improving. An increasing number of surveys (e.g. the Cyber Security Breaches Survey, conducted by Ipsos MORI for the UK Government), as well as the incorporation of cyber 'indicators' into victimisation surveys and police recorded crime have allowed for the development of a

clearer picture of cybercrime trends, particularly in the context of COVID (Buil-Gil *et al*., 2020).

Official recorded crime statistics in Scotland show emerging trends that are potentially indicative of a major transformation in crime. In April 2020, there were 18% fewer offences reported to the police than April 2019. This was driven by large reductions in offences with a characteristic 'physical' component, with violent crime decreasing by 14%, sexual crime decreasing by 26%, shoplifting decreasing by nearly half, and a 29% reduction in 'other theft' (Scottish Government, 2020a). However, for fraud (a criminal offence category under which much volume cybercrime falls) there was a 38% increase on the previous year. The following month (May 2020), saw a reduction of only 5% in criminal offences reported to the police on the previous year, with violent and sexual crimes remaining down on 2019, but a 72% increase in fraud, and a 52% increase in 'other crimes', largely driven by drug possession offences and crimes against public justice, such as bail offences (Scottish Government, 2020b). Although the picture is still emerging, it is not surprising that this data suggests that lockdown in Scotland has had substantial effects on the geographies and patterns of crime. This is mirrored in England and Wales, with an ONS report showing a 23% year-on-year increase in reported cybercrime, including a 55% increase in 'hacking - social media and email' offences and a 61% increase in 'computer virus/malware' offences (Muncaster, 2020). Further evidence regarding the rise of cybercrime has been reported by the Police Service of Northern Ireland (Belfast Telegraph, 2020), and the Scottish Government Cyber Resilience Unit (2020).

Turning to empirical data collection beyond official statistics, we find from the Cambridge Cybercrime Centre's (CCC) analysis of their cybercrime datasets that the social changes and government policies which have emerged as a result of COVID-19 appear to have been exploited by the low-level cybercrime economy. Early analyses suggest this was a result of many users (including adolescents and young adults) being confined to home with no school or work for much of the day. Increased boredom may well be a key driver of online petty crime (Collier, 2020a; Maimon and Howell, 2020). Anxiety over job losses and business closures may prompt some to become involved in or to increase existing illicit online activity as a means of income generation. The CCC has observed significant increases in trading in some ancillary cybercrime markets, such as Paypal and Bitcoin exchanges on cybercrime forums (Vu *et al*., 2020), in Denial of Service attack services (Clayton, 2020), as well as across a range of illicit products, such as stolen accounts. This increase was also observed in online far-right forums (Vu, 2020). This influx of additional money and activity does not appear to represent a *transformation* of online illicit services, volume crime or cybercrime-as-a-service markets, but rather is a general *stimulus* to these markets arising from changes to everyday life brought about by lockdown.

There are also indications of increased opportunities for fraud. Many online frauds reported appear to rely on classic 'social engineering' and deception to elicit a response from victims (Hadnagy, 2010). These techniques are made more salient by social conditions induced by the pandemic. The pandemic has generated a heightened sense of fear and uncertainty, further exacerbated by lockdowns: many people are isolated, separated from friends and extended family, and/or facing lockdown alone. Many will be spending an extended period of time online, working from home, or perhaps engaging with the 24-hour news cycle. Among the fraudulent activities reported is a rise in fake online shop fronts claiming to sell masks, tests, or treatments for COVID, and there is evidence that those who commit cybercrime have adapted the language of their scams rapidly in response to government initiatives. It has also been reported anecdotally that there has been an increase in bogus adverts for pets (including puppies and parrots) on local classified advertising platforms, exploiting people's wish for companionship during extended periods of home-based life and social isolation.

Scams, spam, and phishing campaigns are being adapted, but there are limited indications that this amounts to a true increase in prevalence; rather, COVID-19 is currently being used because it is eye-catching. For many of the more directly-COVID related crime risks, reporting has often stemmed from FBI actions, and so it is important to note that increased prominence of these risks may be a result of greater law enforcement focus on these activities. Much of the public health response to COVID-19 relies on the clear and robust delivery of messages to the public, and the collection of evidence and statistics from individuals (for example, through contact tracing). This in turn relies on digital infrastructure: ranging from online advertisements, information on social media (10DowningStreet, 2020), and online policy announcements through the traditional press (GOV.UK, 2020), to contact detection apps, test and trace portals (NHS UK, 2020). These in themselves present opportunities for emerging cybercrime risks, either from misinformation, fraud, or direct attack.

It would seem that at least in the short term, COVID-19 has been associated with a transformation, not of cybercrime, but of the 'push' and 'pull' factors, routine activities, specific risks, and cultural contexts which feed it. While agencies in the UK have recognised the potential for COVID-19 cybercrime threats, the wider societal changes emerging as a result of the virus and national suppression efforts may lead to more lasting changes in offending and victimisation. This may ultimately require changes to policing practice. In the next section, we examine how COVID-19 has already changed routine activities, before considering how local policing might be adapted.

4. Routine activities in (and following) a pandemic: a generational shift in patterns of crime

The COVID-19 pandemic has led to the construction of new patterns (maybe even a 'new normal') of everyday life and has greatly accelerated a range of wider social and economic transformations that were previously under way such as remote working. In the context of policing, new technologies have been adopted quickly to support the enforcement of new powers and the reshaping of older practices to follow government guidance (see Wells *et al*., 2020). There has only been limited time in which to critically assess the wider practical, security and ethical dimensions of that adoption. Police have necessarily adapted their 'order maintenance' practices as best they can (Reiner, 2010), but they face a fundamental challenge. In this section, we first discuss the short-term effects of strict lockdowns, increased mortality rates, and social panic in the context of the 'first wave' of the virus, and how this may inform our understanding of the early changes to crime which we observe. This may also prove useful in the (not unlikely) event of subsequent waves of this or future viruses. We then look more broadly to what may be the lasting effects of the current pandemic on cybercrime.

The short-term effects of strict lockdowns across much of the world in of the first half of 2020 have been profound. Considering these effects in terms of social ecology and criminal opportunity, we identify a range of ways in which these are driving opportunities for online harm. First, the experience of 'lockdown' prompted a major shift in the social organisation of everyday economic life. Since the closing of non-essential shops, consumers are engaging in more online shopping and businesses and organisations are developing their online presence and capabilities. Some businesses have already declared bankruptcy and others are likely to follow. Organisations have been forced to move online rapidly and adapt to remote and home-based working where possible. Through the lens of 'routine activities' this has significant consequences. In physical and geographical terms, for many the home is now occupied for most of the day while many shopfronts, factories and commercial sites have been unoccupied or experienced reduced occupancy. However, at the same time

(under lockdown conditions), many potential offenders are also confined at home. The prevalence, location, and form that property crime takes is thereby being changed. Equally, the night-time economy (itself associated with substantial amounts of crime and harm) effectively ceased to operate for much of March to July 2020.

Moreover, remote working, online shopping, online entertainment services, online payments, and data processing are being embraced in new ways and at far greater volumes (Brauenstein, 2020), as more and more businesses, workers, and consumers innovate to respond to home-based life and social distancing. The speed with which these technologies have been adopted has not always allowed for the adequate development and provision of cyber security practices or cyber-incident response plans, protocols or training, and potential disruption to home Internet connections (as through Denial of Service attacks, which can be purchased at low cost through 'booter' services) now poses a potentially serious risk to people's working lives. *The New York Times* has reported rapid increases in the number and volume of online payments processed, and large retailers are reporting increases in online sales (New York Times, 2020). Shifts to online shopping have also been innovating at more local levels as small and medium local enterprises seek a sustainable model for an uncertain future. The situation is further compounded by the necessary downloading and use of software with which individuals and employees may be unfamiliar, and on machines that are not centrally administered. This may have knock-on effects on software updating practices (see Vaniea and Rashidi, 2016), the secure storage of personal data, the use of firewalls, and compliance with data protection regulations. Together this rapid and vast techno-social change in everyday life inevitably increases opportunities for or and vulnerabilities to online offending.

These changes also affect the daily lives of those involved in *committing* cybercrime in a range of ways. During periods of lockdown, many adolescents and young people are spending an increased amount of their educational, social, and leisure time online. Even when education and work have resumed, for many, this is unlikely fully to resemble or reflect co-present experience prior to the pandemic. Increased boredom and personal 'strain' which this has caused may be exacerbating the 'push' factors towards involvement in cybercrime and other forms of harmful or illegal online behaviour (Collier, 2020a). Those already involved in cybercrime communities and forums have substantially more time to engage with these activities, while those experiencing unemployment and economic strain may increase their participation in online illicit markets in order to supplement their income. There is evident potential for an increased number of 'willing offenders' who have access to a greater number of particularly vulnerable individuals and businesses.

Our social lives have also rapidly moved online. As people spend more time on social networks and new communication platforms such as Zoom, they are exposed to a wider variety of threats and more often. As platforms become more popular, new threats are likely to emerge (e.g. 'Zoom bombing'). These changes are particularly visible in the rise of virtual classrooms, restricting the social activities of children and young people. This will potentially have significant implications for children and younger Internet users' exposure to cyber-bullying or child sexual exploitation (Interpol, 2020). Equally, parents may be restricted in their ability to exercise oversight, and may be less well connected with organic informal social networks of support and advice (see Rader and Wash, 2015).
Even as lockdowns ease, it is reasonable to suspect that certain far-reaching social-organisational and economic changes, for example to working patterns and online shopping, are likely to persist well into the future. It would be premature to suggest that we have reached a stable 'new normal'; as weeks pass and guidelines shift variably across societies, our 'new normal' is continuously being redefined and renegotiated to the extent that any conceptualisation of 'social order' is necessarily tentative. A number of changes can, however, be observed in our current context that will have implications for people's exposure to online risk, and as a result, demand for policing. Our central aim at this point is to begin

building an argument that peers beyond 'policing during a pandemic' in order to consider the longer-term and deeper social change the pandemic could usher in, the changes in crime patterns we might expect, and the implications of those changes for 'post-pandemic policing'.

Crucially, the early indicators suggest an increasingly *local* dimension to many of the forms of online crime which are on the rise: bullying and harassment, grooming and stalking, fraud, and other forms of victimisation that, despite their digital dimension have distinctly local characteristics, often either involving people living within the same communities and jurisdictions, or interacting with local risks, concerns, and challenges.

5. Local policing of cybercrime: 'reterritorialising' online crime

The current moment appears to be one of *interregnum* and transition to a period in which people's everyday lives and their experiences of crime and harm may look rather different. This raises questions about how societies currently deal with cybercrime, and whether it may be constructive to re-examine its local dimensions.

Our analysis proceeds as follows. First, we explore how the Internet, while global in scope, necessarily remains locally grounded. Second, we argue that while it is vital to recognise cybercrime's international dimensions, there are various ways cybercrime may be rooted in a given locale, and which may be particularly apparent in the context of the COVID-19 pandemic. Third, we demonstrate how certain core activities of cybercrime units within regional police forces already contain local elements, and argue for building further on this capacity and expanding the role of local police in the policing of cybercrime, including in relation to its prevention, detection and investigation. Last, we reflect on the ways local police are already well-placed to build on their existing community-oriented work to tackle cybercrime, and point to some of the challenges that a step-change in and significant upscaling of capacity are likely to present.

The geography of policing (in general) cannot easily be conceptualised simply through a 'local' versus 'global' opposition, and includes important distinctions between international, national, regional and local policing issues (Bowling, 2009). However, in the context of cybercrime, we argue that it is analytically useful to counterpose two distinct sets of issues which cut across these geographies. The first of these are 'globalised' cybercrime policing issues, which address predominantly issues of jurisdiction, sovereignty, and the mass-scale interconnection of people and services remotely around the world (for a more comprehensive review see Holt et al., 2015). These issues are fundamentally about the ways in which the Internet further complicates and challenges the sovereign geography of state power (Garland, 1996). These policing challenges have been well articulated elsewhere (see Yar and Steinmetz, 2019), and will only receive a brief mention here. At a national and international level, public policing and the conventional criminal justice apparatus is required to engage in increasingly complex public and private co-operation (see for example Levi and Williams., 2013). These efforts may be enabled or frustrated by international relations and the dynamics of geopolitical power (Cavelty, 2007). Additional issues are presented by private sector platforms and service providers whose position in the Internet's social and technical infrastructure shape the existential security of the nation state and support or undermine its claim to sovereignty over its citizens (Brodeur, 2010; Collier, 2020b). The second set of issues, in contrast, and which we foreground in this paper, are 'localised' issues, in which the Internet's interpenetration of local infrastructures, cities, towns, and communities connects individuals within local geographies in novel ways (for example Miller, 2015). In these regional and community policing contexts, social harms need to be understood with reference to specific knowledge about these local communities and

their needs, through partnerships in which issues of trust and legitimacy are crucial (Mackenzie and Henry, 2009).

While the Internet enables the international flow of data between connected computing devices, it ultimately involves users and computers that are physically located in specific places. In order to deliver low-latency and localised services to users, the architecture of the Internet, and in particular the geographic location of network servers, may often be physically situated close to a certain region, cluster of users, or locale, meaning that 'gamers' using an apparently international gaming service, for example, may in fact have their sessions hosted on a server alongside other local users. That is to say that people playing in Scotland, for instance, may be sorted into online games with other players in that and neighbouring countries. Furthermore, the architecture of the Internet shapes access to services. Wealthier countries and regions are able to invest more in infrastructure, and faster networks tend to be located in urban centres. The geography of the Internet has drawn significant research attention due to its uneven lines of distribution, access, and control *(*Graham, Ojanpera, and Dittus, 2019*)*. As a result of a mixture of technical (e.g. low latency), legal/regulatory, and economic reasons, network servers and services may be situated relatively close to end users. Emerging paradigms such as 'edge computing' - a networking concept with the philosophy that *"*computing should happen as close as possible to the data source*"* (Shi *et al*., 2016) - appear set to amplify this process. The increased deployment of edge computing (for example in support of smart cities or Internet of Things (IoT) devices) means that users are increasingly likely to be served by closer computational resources. This ultimately places our online lives increasingly proximate to our physical location.

Cybercrime may also exhibit 'local' qualities in a number of respects. The localisation of network servers and computing resources may generate scenarios in which both the cybercrime offender and victim, as well as key elements of the network, are all geographically proximate (Collier et al., 2019). Various forms of online harassment are likely to involve an offender already known to the victim, or who is a member of a particular known local community, even if the platform on which the offence takes place is provided by a global social media company. Intimate partner violence is a particularly important case of this form of crime with an increasingly 'online' dimension (Lopez-Neira *et al*., 2019). Regardless of the physical location of servers, certain forms of cybercrime may involve distinctively 'local' dimensions, as a result of shared (or disputed) politics, languages and culture. Even where the victim and offender are not local to one another, and where there is no obviously single 'local' dimension to the offence, offender and victim nevertheless both reside in a specific district in a specific country, and there is therefore scope for their respective local police forces to become involved. As we discuss further below, this scenario is in fact effectively the backbone of the policing of cybercrime to date, including in relation to Child Sexual Abuse Material (CSAM), computer 'hacking', and malware, among other types of cybercrime.

We have argued thus far that the COVID-19 pandemic has accelerated the migration toward online services, modified computer users' real-world and online routine activities, and introduced new cyber security vulnerabilities. As routine activities shift in the pandemic to bring forms of activity such as shopping and socialising more fully 'online', whilst some of this will abandon local locales in favour of the lower costs and larger communities afforded by national and international platforms, we may predict that other local retailers, services and communities will embrace and thrive online, and thus so too will the cybercrime risk landscape take on an increasingly local character. As the public become increasingly exposed to cybercrime risks in the context of the pandemic, clarity around the police role in responding to and preventing cybercrime is essential. The pandemic presents local police services with an opportunity to go beyond orthodox approaches to cybercrime prevention - and we argue that they are in fact particularly well-placed to do so. The role of public policing in responding to cybercrime is however currently relatively small in comparison with the

private and non-governmental sectors and with more centralised policing agencies such as the NCA (Wall, 2007).

The present paucity of the local police role in responding to cybercrime is generally explained through the practical limitations imposed by the supposedly global and immaterial nature of online life (see Wall, 2007: 162-165), and/or the cultural construction of cybercrime and the police role. The scale of common forms of cyber-victimisation both in number of victims and geographical spread challenge geographically-bounded regional force capacities. Where individual harms are minor, and resources are stretched, questions are raised in local forces about whether it is in the public interest to devote resources to costly multi-national investigations. . On the one hand, police occupational culture's embedded notions of 'danger' and concern with 'crime-fighting' and 'emergency response' (Reiner 2010, 1979; Skolnick 1966) mean that many common forms of cybercrime do not neatly fit into that role, despite evidence of perceived seriousness or claims of ownership of the crime problem (Bossler et al., 2015). On the other hand, low reporting levels contribute to a limited police mandate to address cybercrime, and has been explained by the public's perception of common cybercrime as an individual problem which passes the threshold for police action in only a limited number of instances (HM Government, 2016; Yar, 2013). The police face additional problems of sufficient training (Reform, 2017; Cockcroft et al., 2018), and ultimately retaining trained officers where salaries struggle to compete with the offerings of the private sector (Harkin et al., 2018; Whelan and Harkin, 2019). While an increasing number of authors are exploring the new and innovative ways police are responding to a variety of cybercrime threats (Brewer et al., 2019; Dupont, 2016), we argue that at the level of local policing more attention has been paid to its limits than its capacities and possible futures.

We are not suggesting that regional police forces can or should take on primary responsibility for 'responding' to volume cybercrime, nor alone pursue or duplicate costly and complex investigations amidst the pandemic. Instead, we propose that now is a key moment in which the public police can carve out and assert its role in the prevention and policing of cybercrime locally. For the current discussion, we separate this preventive role into two main strands, with one strand focused on victims, potential victims, and communities and the other focused on offenders. These should be understood as 'ideal types' for the purpose of argument and conceptual analysis, rather than a prescriptive reduction of the complexities of the public-police role.

The first of these roles involves engagement with victims (and potential victims) of cybercrime including crimes such as fraud, online grooming and harassment. In a review of the evidence on cyber security awareness campaigns, Bada *et al*. (2015) argue that in order to be effective, cyber awareness messages and their communication need to resonate with their target populations. Who communicates messages and how these messages are conveyed will shape how the target audience interprets and operationalise their recommendations. Current provision within the UK, for example, is UK-wide in its orientation and pursues a 'top-down' strategy of effectiveness by simplicity and consistency. In approaching cyber resilience in this way however, the messages cannot account for diverse social and cultural contexts, which leave them vulnerable to misinterpretation (Horgan, 2019).

The second strand of this preventive role targets those who commit, or are at risk of committing, cybercrime and the online communication offences we discuss above. In this case, for criminal conduct which involves very large numbers of often low-level offenders, target hardening from security companies is largely unhelpful, and the investigative capacities of centralised LEAs are more suited to small numbers of individuals and groups involved in limited-scope, high-harm offending. However, police services are uniquely well-placed to engage with these forms of crime due to their existing human infrastructure and

skills, deep ties to local communities, and knowledge of local issues. The police already deal with much interpersonal online crime through their regular duties, despite its 'online' dimension - however digital spaces are often perceived by the public (and sometimes the police) to be outside routine police-work.

Of course, policing is no stranger to issues of centralisation and its implications for effective and accountable local policing - issues that have been debated in Scotland in recent years, for example (Henry, 2017; Jones, 2008). Arguably, it is in finding the balance between centralised and localised responses that policing might best advance (Henry, 2017). Thus far, discussions of cyber security and cybercrime prevention strategies have reflected the very global and inter-jurisdictional conditions which tend to underlie most approaches, however here we argue that issues of localism and local responsiveness are long overdue development and integration. If we are to proceed with a 'responsibilisation strategy' (Garland, 2001) geared towards population-level behaviour change, harnessing the specific knowledge and community networks that local policing has developed and is concerned with promoting is one way that central messages can be communicated to different groups in ways that are sensitive to and engage with their local social and cultural contexts. It is important to note that here we are making a distinction between community-level engagement with individuals deemed 'at risk' of offending captured by the work of the NCA, and the more discursive, problem-solving and participatory approaches to policing that help identify the specific challenges and needs present in local communities (Skogan, 2006).

If a case is to be made for an increased role of local police in cybercrime policing, this also presents an opportune moment for consideration as to what would be the ideal characteristics of that role. At the heart of this re-envisioning of the police's role is the incorporation into cybercrime policing of core 'process-led' community policing principles such as 'citizen-involvement', 'problem solving' and 'decentralisation' (Skogan, 2006) on the one hand, and core principles of 'democratic policing' on the other (Jones, 2008: 694-697), including 'responsiveness', 'participation', 'information', and 'equity'. This approach serves to help construct cybercrime and cyber-resilience as local issues around which communities of support can be mobilised to enhance collective efficacy. By inviting community stakeholders to have conversations about cybercrime, they can become part of a dialogue in which they have an active stake, rather than simply being the subjects of top-down uni-directional awareness campaigns. Beyond addressing the weaknesses of 'one-size-fits-all' awareness campaigns through facilitating these kinds of conversations, local police services are in a better position to encourage reporting, challenge the stigma associated with victimisation (Button and Cross, 2017), and capture a more reliable picture of cybercrime victimisation within different communities. Arguably, local frontline police are in a unique position to undertake this work and reinforce cybercrime prevention in a way that extends beyond yet complements the remits of centralised agencies.

Public police have already been developing community partnerships of this kind, particularly with small and medium-sized enterprises (SMEs) and third sector organisations. In Scotland, to establish a dialogue between businesses who may be the target of cybercrime, Police Scotland and the Scottish Business Resilience Centre (SBRC) developed a leaflet promoting cyber security (Scottish Business Resilience Centre, 2020). Other forces have taken a different approach to engage with the SME community. In partnership with the London Digital Security Centre (LDSC), uniformed police officers visit these businesses to build up a relationship, promoting who can be contacted in the event of cyber security issues (Bada and Nurse, 2019). Hampshire Constabulary worked in association with the University of Portsmouth to explore how to increase cyber resilience and cyber-awareness within the wider community (Karagiannopoulos *et al*., 2019). The work draws several conclusions, focussing on different dimensions of a community, e.g. young people, the elderly, the general public, and SMEs. This approach to engagement could be rolled out on a wider scale, complementing existing work carried out by local police.

It is important to emphasise that we are not arguing for the local police to simply extend the intelligence-gathering arm for high-policing functions, or to become a localised PREVENT-style service. Rather, the principles of democratic and community-oriented policing point to a potential set of values to be embodied by 'low' cybercrime policing functions which might have particular purchase for addressing volume cybercrime victimisation as an issue. Here we propose that in constructing cybercrime as a local policing issue, we are inviting it to be subjected to the lens of democratic (Jones, 2008) and community-oriented models (Skogan, 2008), of both police response and scrutiny.

While community policing is a contested term both in philosophy and practice (Skogan, 2006), the activities that fall under its rubric (and its concern with building working relationships and legitimacy) render it a desirable feature of the policing of cybercrime for a number of reasons. For analytical exposition we can take Skogan's (2006) core principles as a starting point, namely that community policing is a process dedicated to citizen involvement, problem solving, and decentralisation. Contemporary centralised approaches to cybercrime policing (Scottish Government, 2018; HM Government, 2016) certainly engage in 'problem-solving' and 'citizen involvement'. However, these engagements appear limited to private and public sector entities (SMEs and large businesses), with less attention paid to engaging communities (geographically or culturally local and proximate) in dialogue about their experience of cybercrime, and how they might be involved in the development of policing. Centralised forms of cybercrime policing are facilitated in the context of businesses through umbrella organisations and their capacity cascade information. Equally, it is acknowledged in government and policing strategies (Scottish Government, 2018; HM Government, 2016) that different public and private sector sub-sections have different policing needs, much like the varying needs of different communities. The Scottish Household Survey (2019) illustrates how engagement with 'cybersecurity' varies with age and socio-demographic status suggesting that a more target and community-oriented approach is needed. - . Without emphasising community involvement, policing risks merely becoming the enforcement of compliance, with communities subject to top-down policing interventions in which they have little active engagement or stake. We argue that the existing infrastructure of relationships and practices which make up community policing might usefully allow this kind of work and engagement.

We acknowledge that community policing is not without its challenges. Community policing is founded on an assumption that sufficiently coherent and homogenous 'communities' that share or agree upon collective needs and priorities, and a community-oriented policing of cybercrime will need to build on existing community relationships to establish where policing cybercrime needs are present and distinctive. 'Communities' seldom manifest in such uncomplicated formations. As Henry (2017) points out in the context of traditional policing, 'engagement' without 'equity' risks policing activity that reflects the loudest or most privileged voices, missing those who need support. In conventional modes of policing, engagement efforts may be further frustrated by difficulty in reaching certain groups who may not have capacity or desire to engage in dialogue with policing organisations. Arguably, in the context of cybercrime, this frustration may be a function of cultural constructions of police and cybercrime mentioned earlier; as emergency responders dealing with immediate danger. Conversely, it may be that by emphasising community engagement and dialogue about cybercrime policing needs, local police can rearticulate their role in a way that incorporates the local experience of cybercrime. Despite these acknowledged challenges, we argue that re-envisioning cybercrime as a community policing issue is worthwhile. Local forces have the resources and connections to tailor interventions that are 'responsive' to local-community needs, can be explained to the public, and can be held accountable through democratic mechanisms (Jones, 2008; Henry, 2017; Brodeur, 2010). Engaging local communities in problem-solving dialogue focused on cybercrime is a task for which we would suggest conventional local police are ideally suited. This may resultantly create a democratic arena

for debate, empowering the public to challenge some of the assumptions around how cybercrime is currently policed at the local level. This may move the governance of cybersecurity from a primarily unidirectional, top down approach situated either in central government entities or under the stewardship of private Internet platforms, to a dialogical one which draws on the knowledge of both territorial police leadership and frontline officers, as well as the local communities themselves. While the digital dimension of local crime, and the local dimension of digital crime, already form a part of police duties, we argue that the pandemic has created a need for the mainstreaming of this 'local digital policing' as a core part of the frontline police role.

6. Conclusions: The social ecology of cybercrime in an era of mass social change

COVID-19 induced changes in routine everyday life are contributing to a wider transformation in cybercrime. We propose an alternative vision for the role of the public police in a society that is likely to experience an increase in the number of cybercrime victims and offenders that fall within its terrestrial borders. The literature on policing cybercrime has consistently reproduced an account of this role that has become a somewhat unchallenged orthodoxy; public police capacity to address cybercrime is limited by its global nature, the geographical limits of police jurisdictions, the complications and costliness of transnational investigations, constraints on resources, and the values embedded in 'police culture' about 'real police-work' (Yar and Steinmetz, 2019; Boes and Leukfeldt; 2016; Yar, 2013; Wall, 2007). These arguments have been further buttressed by the persistent underlying construction of cybercrime policing and cyber security as a private problem with privatised solutions, the provision of which has been predominantly left to the free market (Yar, 2008).

Due to ongoing societal changes that have been accelerated by the COVID-19 pandemic, it is critical that we re-evaluate this position. We make the case that by reconstructing cybercrime and cybercrime prevention as a local public policing issue, the public police can reassert their role in policing cybercrime in a way that addresses inherent weaknesses in centralised approaches. By virtue of territorial forces' local policing infrastructure and their guiding principles (Police Scotland, 2020), their community and front-line officers are in a unique position to carve out this role. This ultimately complements more centralised efforts in a way that is responsive to the local needs of different communities in a way that the private sector and national 'high-policing' agencies may not always be able to do.

This is an ideal moment for local police forces to reexamine how they will pursue cybercrime policing in a way that is sustainable and reflects the monumental social and economic changes we have witnessed in recent months (but which are likely to stay with us). There are clear cybercrime threats and risks directly linked to COVID-19 which will benefit from police engagement with specialist agencies, including at the national or even international level, which have the capacity for advanced digital forensics and targeted cybercrime operations. However, as local policing is structured around local policing teams, we believe there is significant opportunity for the local policing of cybercrime similar to upscale or broaden the role of these teams to engage communities, businesses, organisations and stakeholders, inlduing children, young people, and vulnerable adults, in conversations about cybercrime, their specific needs and challenges. Much of this is work in which frontline police are already engaged; however, we suggest that cybercrime problems be incorporated as a core part of this frontline role.

In doing so, a democratic approach to the local policing of cybercrime and online harm may promote greater participation, enhance responsiveness, and contribute to an equity of service for individuals that is unrealistic via a centralised approach (or via private Internet

companies and platforms). This would allow local policing to capitalise on the existing relationships and insights long-developed in specific localities, link up awareness messaging with its target audience(s) in more direct ways, and enhance the legitimacy of both the messages and the public police as cybercrime responders. By enhancing the efficiency and responsive targeting of resources through the collection of frontline community intelligence and measurement of outcomes and local capacities, both police and researchers can better evaluate these approaches on an ongoing basis. In the interim, we argue that territorial police forces should review their cybercrime policing and prevention practices and capabilities to assess their current adequacy and resilience.

We have approached an ideal moment in which to consider revising the public policing of cybercrime. Too much attention has been focused on the limits of the public police capacity, and not enough attention paid to its strengths or potential to play a unique and complementary role in tackling cybercrime. Arguably, the skills and capacities of local police will be crucial in responding to cybercrime and promoting equitable access to greater cyber security and justice.

7. References

10 DowningStreet (2020), “To keep the virus under control, we all need to follow the rules: wash our hands, cover our faces and make space.” [Twitter]. 1 August 2020. available at: https://twitter.com/10DowningStreet/status/1289533770303856641 (accessed 13 August 2020)

Bada, M., Sasse, A. and Nurse, J. (2015), “Cyber Security Awareness Campaigns: Why do they fail to change behaviour”, *Proceedings of the International Conference on Cyber Security for Sustainable Society*, available at: https://arxiv.org/abs/1901.02672 (accessed 27 May 2020)

Bada, M., & Nurse, J. R. (2019), “Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs)”, *Information & Computer Security*, Vol. 27 No. 3, pp.393-410.

Behr, H. (2008), “Deterritorialisation and the transformation of statehood: The paradox of globalisation”, *Geopolitics*, Vol. 13, No. 2, pp.359-382.

Belfast Telegraph (2020), “Police Warn Businesses of Cyber Crime ‘Surge’ During Lockdown”, *Belfast Telegraph*. available at: https://www.belfasttelegraph.co.uk/news/northern-ireland/police-warn-businesses-of-cyber-crime-surge-during-lockdown-39151612.html (accessed 22 May 2020)

Boes, S. and Leukfeldt, E. (2016), “Fighting cybercrime: A joint effort”, Clarke, R. and Hakim, S. (Eds) *Cyber-Physical Security*, Springer, London, pp.185-203.

Bowling, B. (2009). Transnational policing: The globalization thesis, a typology and a research agenda. *Policing: A Journal of Policy and Practice*, 3(2), 149-160.

Brewer, R., De Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). Cybercrime prevention: Theory and applications. Springer Nature.

Brodeur, J.P. (2010), *The Policing Web*, Oxford University Press, Oxford.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020), 'Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK', *European Societies*, pp.1-13.

Button, M. and Cross, C. (2017), *Cyber Frauds, Scams and their Victims,* Routledge, London.

Cavelty, M. D. (2007). Cyber-security and threat politics: US efforts to secure the information age. Routledge.

Clayton, R. (2020), The impact of lockdown on DoS-for-hire, *CCC Briefing Paper series,* available at*:* https://www.cambridgecybercrime.uk/COVID/COVIDbriefing-3.pdf (accessed 18 August 2020)

Clayton, R., Moore, T., & Christin, N. (2015, June). Concentrating Correctly on Cybercrime Concentration. In WEIS.

Cockcroft, T., Shan-A-Khuda, M., Schreuders, C. and Trevorrow, P. (2018), 'Police Cybercrime Training: Perceptions, Pedagogy and Policy', Policing: A Journal of Policy and Practice

Cohen, L.E. and Felson, M. (1979), "Social Change and Crime Rate Trends: A Routine Activity Approach", *American Sociological Review*, Vol. 44, No. 4, pp.588-608.

Collier, B. (2020a), Boredom, routine activities, and cybercrime during the pandemic, *CCC Briefing Paper series,* available at: https://www.cambridgecybercrime.uk/COVID/COVIDbriefing-4.pdf (accessed 13 August 2020)

Collier, B. (2020b). The power to structure: exploring social worlds of privacy, technology and power in the Tor Project*. Information, Communication & Society, 1-17.*

Collier, B., Horgan, S., Jones, R., and Shepherd, L. "The implications of the COVID-19 pandemic for cybercrime policing in Scotland: A rapid review of the evidence and future considerations.", Scottish Institute for Policing Research, Research Evidence in Policing: Pandemics Briefing Paper (2020).

Collier, B., Thomas, D.R., Clayton, R. and Hutchings, A. (2019), "Booting the booters: evaluating the effects of police interventions in the market for denial-of-service attacks", *Proceedings of the Internet Measurement Conference*, October 2019, pp.50-64.

Dupont, B., (2016), "Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime", Crime, Law and Social Change, Vol. 67, No. 1. p.97-116
Garland, D. (2001), *The Culture of Control*, Oxford University Press, Oxford.

Garland, D. (1996). The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society, The British Journal of Criminology, 36(4), 445-471.

GOV.UK (2020), "Coronavirus (COVID-19)", available at: https://www.gov.uk/coronavirus (accessed 13 August 2020)

Graham, M., Ojanpera, S. and Dittus, M. (2019), 'Internet Geographies: Data Shadows and Digital Divisions of Labour', in Graham, M. and Dutton, W.H. (eds) *Society & The Internet* (2nd ed), Oxford University Press, Oxford.

Guardian (2020), “Hacking attacks on home workers see huge rise during lockdown”, 24 May 2020, available at: https://www.theguardian.com/technology/2020/may/24/hacking-attacks-on-home-workers-see-huge-rise-during-lockdown (accessed: 27 May 2020)

Hadnagy, C. (2010), *Social Engineering: The Art of Human Hacking*, Wiley Publishing, Inc., Indianapolis, IN.

Harkin, D., Whelan, C. and Chang, L. (2018) “The challenges facing specialist police cyber-crime units: an empirical analysis”, Police Practice and Research, Vol. 19, No. 6, pp: 519-536

Henry, A., & Mackenzie, S., (2009). “Community Policing: A Review of the Evidence”, The Scottish Government. available at: https://www.research.ed.ac.uk/portal/files/13387749/Henry_A._Mackenzie_S._2009_._Community_Policing_A_Review_of_the_Evidence.pdf (Accessed 20 Oct 2020)

Henry, A. (2017), “Police governance and accountability”, *Policing 2026 Evidence Review*, Scottish Institute for Policing Research, pp.89-104, available at: https://www.research.ed.ac.uk/portal/en/publications/police-governance-and-accountability(e8739bad-696b-4d6f-b525-03dc4397cadc)/export.html (accessed 27 May 2020)

HM Government (2016). National Cyber Security Strategy 2016-2021. London: HM Government.

Holt, T.J. and Bossler, A.M. (2008), “Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization”, *Deviant Behavior*, Vol. 30, No. 1, pp.1-25.

Holt, T. J., Burruss, G. W., & Bossler, A. (2015). Policing cybercrime and cyberterror.

Horgan, S. (2019), *Cybercrime and Everyday Life*, Doctoral thesis, University of Edinburgh, Edinburgh, UK.

Interpol (2020), Interpol Report Highlights Impact of COVID-19 on child sexual abuse, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse

Jones, T. (2008), “The Accountability of Policing”, Newburn, T. (Ed.) *The Handbook of Policing* (*1st edition*), Willan Publishing, Cullompton, UK, pp.693-724.

Karagiannopoulos, V., Sugiura, L. and Kirby, A.L. (2019), *The Portsmouth Cybercrime Awareness Clinic Project: Key Findings and Recommendations*, University of Portsmouth, Portsmouth.

Leukfeldt, R. and Yar, M. (2016), “Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis”, Deviant Behaviour, Vol. 37, No. 3, pp 263-280

Levi, M., & Williams, M. L. (2013). Multi-agency partnerships in cybercrime reduction. Information Management & Computer Security.

Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., & Tanczer, L. (2019). ‘Internet of Things’: How abuse is getting smarter. Safe – The Domestic Abuse Quarterly, (63), 22-26.
Mackenzie, S., & Henry, A. (2009). Community policing: A review of the evidence. Scottish Government.

Maimon, D., & Howell, C. J. (2020). The coronavirus pandemic moved life online – a surge in website defacing followed. The Conversation.

McGuire, M. (2007), Hypercrime: The New Geometry of Harm, Routledge Cavendish, Oxon.

Miller, D. (2016). Social media in an English village. UCL Press.

Muncaster, P (2020), "Cybercrime Jumped 23% Over Past Year, Says ONS", *Infosecurity Magazine*, available at: https://www.infosecurity-magazine.com/news/cybercrime-jumped-23-over-past-year/ (accessed 13 August 2020)

Newman, G. and Clarke, R. (2003), *Superhighway Robbery: Preventing e-commerce crime*, Wilan, London.

New York Times (2020), "Amazon sells more, but warns of much higher costs ahead", available at: https://www.nytimes.com/2020/04/30/technology/amazon-stock-earnings-report.html (accessed 27 May 2020)

Police Scotland (2020), "COVID-19 - Police Scotland Response", available at: https://www.scotland.police.uk/about-us/covid-19-policescotlandresponse/ (accessed 27 May 2020)

Rader, E. and Wash, R. (2015), "Identifying patterns in informal sources of security information", *Journal of Cybersecurity,* Vol. 1, No. 1, pp.121-144.

Reyns, B.W. (2018), "Routine Activity Theory and Cybercrime", Steinmetz, K. and Nobles, M. (Eds.), *Technocrime and Criminological Theory*, Routledge, London

Reiner, R. (2010), *The Politics of the Police* (4th edition), Oxford University Press, Oxford.

Reform (2017). Bobbies on the Net: A Police Workforce for the Digital Age. London: Reform

Scottish Business Resilience Centre (2020), "Cyber Security: Guide for Small Businesses", available at: https://www.sbrcentre.co.uk/services/cyber-security-guide-for-small-businesses/ (accessed 28 July 2020)

Scottish Household Survey, (2019) SHS Annual Report, https://www.gov.scot/publications/scottish-household-survey-2019-annual-report/

Scottish Government (2020a), "Recorded crime in Scotland: April 2020", available at: https://www.gov.scot/publications/recorded-crime-scotland-april-2020/ (accessed 13 August 2020)

Scottish Government (2020b), "Recorded Crime in Scotland: May 2020", available at: https://www.gov.scot/publications/recorded-crime-scotland-2020/ (accessed 13 August 2020)

Scottish Government Cyber Resilience Unit (2020), 'Cyber Resilience COVID-19 Bulletin', available at: https://blogs.gov.scot/cyber-resilience/2020/05/06/cyber-resilience-notice-covid-19/ (accessed: 22 May 2020)

Shi, W., Cao, J., Zhang, Q., Li, Y. and Xu, L. (2016), "Edge computing: Vision and challenges", *IEEE internet of things journal*, Vol. 3, No. 5, pp.637-646.

Skogan, W. (2006), *Police and Community in Chicago: A tale of three cities*, Oxford University Press, Oxford.

Skolnick, J., (1966), “Sketch of the Policeman's "Working Personality", Cole, G. and Gerz, M. (eds) Criminal Justice System: Politics and Policies (7th ed), Wadsworth, Belmont, CA.

Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society. SAGE Publications Limited.

Vaniea, K. and Rashidi, Y. (2016), “Tales of Software Updates: The process of updating software”, *Proceedings for Computer Human Interaction (CHI) 2016*. ACM, Computer Human Interaction (CHI) 2016, San Jose, United States, 9/05/16.

Vu, A. (2020), The pandemic as incels see it, *CCC Briefing Paper series,* available at: https://www.cambridgecybercrime.uk/COVID/COVIDbriefing-5.pdf (accessed 18 August 2020)

Vu, A., Hughes, J., Pete, I., Collier, B., Chua, Y.T., Shumailov, I. and Hutchings, A. (2020), Turning Up the Dial: the Evolution of a Cybercrime Market Through Set-up, Stable, and Covid-19 Eras, *Internet Measurement Conference, IEEE*

Wall, D. (2007), Cybercrime: The Transformation Crime in an Information Age, Polity Press, Cambridge.

Wells, H., Aston, L., O’Neill, M. and Bradford, B. (2020), “The rise of technologically-mediated police contact: the potential consequences of ‘socially-distanced policing’”, *British Society of Criminology Policing Network,* available at: https://bscpolicingnetwork.com/2020/04/29/the-rise-of-technologically-mediated-police-contact-the-potential-consequences-of-socially-distanced-policing/ (accessed 18 August 2020)

Whelan, C. and Harkin, D., (2019) “Civilianising specialist units: Reflections on the policing of cyber-crime”, Criminology and Criminal Justice, Online First (accessed 20 Oct 2020)

Williams, M.L. (2016), “Guardians Upon High: An application of routine activities theory to online identity theft in Europe at the country and individual level”, *British Journal of Criminology*, Vol. 56, No. 1, pp. 21-48.

Yar, M. (2005),. “The Novelty of ‘Cybercrime’ An Assessment in Light of Routine Activity Theory”, *European Journal of Criminology*, Vol.*2,* No. 4, pp. 407-427.

Yar, M. (2008), “Computer Crime Control as Industry: Virtual insecurity and the market for private policing”, Aas, K.F., Gundhaus, H. and Lomell, H. (Eds), *Technologies of InSecurity*: *The Surveillance of Everyday Life*, Routledge, London, pp. 203-218.

Yar, M. (2013), “The Policing of Internet Sex Offences: Pluralised governance versus hierarchies of standing”, Policing and Society, Vol. 23, No. 4, pp.482-497.

Yar, M.and Steinmetz, K. (2019), *Cybercrime and Society (3rd edition)*, Sage Publications, London.